

EXHIBIT G

Declaration of Philip P. Mann

Case No. 21-CV-0817-TSZ



Video Game Cheating
Expert Witness Report
of
Mr. Steven Guris
for
Perkins Coie LLP

Client Confidential

Client Confidential

Table of Contents

Introduction	2
Qualifications	3
Compensation	4
Summary of Opinions	4
Background & Opinions	5
Background	5
General Definitions and Categorization	5
Genre- & Destiny 2-specific Terminology	6
Game Devices and Digital Download	9
Technical Terms	10
Importance of Viral Marketing	11
Game Ecosystem Investment	12
Game Setting and Suspension of Disbelief	12
Long Term Player Investment	13
Microtransactions and Cosmetic Purchases	14
Security Relationships	15
Cheating in Video Games	16
The Anatomy of a Modern Cheat	17
Relevant Terminology	17
AimJunkies Cheat Loader Download and Installation	19
AimJunkies Cheat Loader: Static Analysis	21
AimJunkies Cheat: General Inferences	24
AimJunkies Loader Dynamic Analysis and Reverse-Engineering	26
Game Product Devaluation	29
Conclusion	31

Client Confidential

Introduction

1. I have been retained as an expert by Bungie, Inc. ("Bungie") to provide my report and testimony in connection with the litigation titled *Bungie, Inc. v. AimJunkies.com, et al.*, No. 2:21-cv-811 before Hon. Thomas S. Zilly at the United States District Court for the Western District of Washington.
2. I have been asked to provide my opinion regarding the video game industry, video game gameplay, and the impact of video game cheats on video games and the video game industry, as well as my technical knowledge of general modern video game cheat operation and the investigative work I have done on the AimJunkies loader specifically.
3. I have been asked to provide this expert report to lay out my opinions on the matter in dispute.
4. The opinions set forth in this report are based on my expertise related to video games and Bungie's *Destiny 2*, as well as my professional experience as an active investigator in digital forensics and cybercrime, and my review of the following documents:
 - BUNGIE_WDWA_0000469
 - BUNGIE_WDWA_0000602
 - BUNGIE_WDWA_0000606
 - PDG_0048
 - PDG_0049
 - PDG_0050
 - PDG_0052
 - PDG_0053
 - PDG_0054
 - PDG_0055
 - PDG_0056
 - PDG_0057
 - PDG_0058
 - PDG_0059
 - PDG_0060
 - HAHN_0000001
 - HAHN_0000004
 - HAHN_0000007
 - HAHN_0000010
 - HAHN_0000013
 - HAHN_0000016
 - HAHN_0000019
 - HAHN_0000022
 - HAHN_0000025
 - HAHN_0000028
 - HAHN_0000031

Client Confidential

- HAHN_0000035
- HAHN_0000038
- Rogers, Everett M.; Larsen, Judith K., Silicon Valley Fever: Growth of High-technology Culture, 1985.
- <https://www.marketwatch.com/story/videogames-are-a-bigger-industry-than-sports-and-movies-combined-thanks-to-the-pandemic-11608654990>
- <https://www.statista.com/statistics/499703/share-consumers-ever-play-video-games-by-age-usa/>, Vorhaus Digital Strategy Study 2022, p. 91.
- <https://www.statista.com/statistics/190225/digital-and-physical-game-sales-in-the-us-since-2009/>
- <https://www.trade.gov/ecommerce-frontline-social-media-forecast>
- <https://www.indeed.com/hire/job-description/community-manager>
- <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100544310>
- <https://www.jstor.org/stable/j.ctv1hp5hqw.13>
- <https://www.bungie.net/7/en/legal/sla>
- <https://support.microsoft.com/en-us/topic/june-28-2022-kb5014666-os-builds-19042-1806-19043-1806-and-19044-1806-preview-4bd911df-f290-4753-bdec-a83bc8709eb6>
- <https://support.microsoft.com/en-us/topic/july-12-2022-kb5015807-os-builds-19042-1826-19043-1826-and-19044-1826-8c8ea8fe-ec83-467d-86fb-a2f48a85eb41>
- <https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/how-user-account-control-works>
- <https://www.virustotal.com/gui/file/2abae185fc87476e00e45c7d3a171a4a2c0a57d714b03608dc566c988ca6ee48/detection>
- <https://www.virustotal.com/gui/file/f2c08cec764e85a42888250cf79747c47b3a7614199f2b4cba98b8745bb7749c/detection>
- <https://kotaku.com/diablo-immortal-p2w-pvp-broken-blizzard-rite-exile-1849355846>, titled: "Diablo Immortal Player Says He Can't Get A Match After Spending \$100,000."

Qualifications

5. I am the Director of Threat Investigations of Unit 221B, a cybersecurity firm contracted by Bungie to investigate cheats and their developers.
6. Until my present appointment, which began August 1, 2022, I had been employed by Unit 221B beginning in 2020 as a Cybersecurity Analyst. From January 2022 until August 1, 2022, I served as the Lead Project Engineer for Networking Testing and Development and as a Senior Investigator within the Investigations division. From August 1, 2022 until September 1, 2022, I served as the Tactical Operations Manager for the Investigations, Network Testing, and Development branches of Unit 221B.
7. As part of my responsibilities for Unit 221B, I lead and conduct investigations into fraud, abuse, and other cybercrime; conduct and lead vulnerability assessments and penetration tests; and spearhead internal development of new software offerings.

Client Confidential

8. I hold a BSc in software engineering from Kennesaw State University.
9. I have personally played countless hours of video games. I had been a player of Bungie's *Destiny 2* prior to my initial hiring by Unit 221B and continue to play *Destiny 2* in my personal time, with over 2000 hours of active play time currently applied to my account.
10. Through my experience and education, I am familiar with video game design, infrastructure, and play.

Compensation

11. I am being compensated for my time at a rate of \$750 per hour for time expended reviewing this matter and for providing testimony or other opinions. My compensation in no way depends on the outcome of this opposition.

Summary of Opinions

12. Bungie's *Destiny 2* is a first-person looter-shooter massively multiplayer online game, extensively marketed through social media and other online mechanisms. Bungie actively participates in their player community through designated Community Managers, company-hosted streams, and other player outreach activities.
13. *Destiny 2* is frequently the subject of organic social media advertising by fans of the game and content creators (generally streamers) whose positive statements and feelings about the game provide incentive for more gamers to choose to play *Destiny 2*.
14. *Destiny 2* is a live-service game, following the "Software as a Service" model. New content expansions and cosmetic upgrades are made available for purchase at regular intervals following the initial release of the game to allow for greater player investment and continued interest. This "microtransaction" model, common to many modern video games, relies upon this player investment and interest for continued revenue from the game; and requires significant ongoing investment by the studio to maintain.
15. Bungie has a security commitment to its players to provide a fair and balanced game environment where the success of a player is defined by the investment of their time and effort on skill-building and gameplay.
16. The presence of cheaters within this environment damages Bungie, poisons the well for players and content creators, and creates an unsustainable and unsafe environment for legitimate players. People who have invested their time, effort, and money into the game will be prevented from completing in-game goals and activities by the presence of these cheaters, driving down player engagement, new player acquisition, and long-term player retention.
17. Modern cheats for live-service games are also dangerous to the user. Installation instructions provided by cheat developers instruct users to perform unsafe and ill-informed configuration changes to their devices that immediately put them at higher risk of malware infection or data theft. Continued operation of a cheat exposes users to this risk whenever the cheat is run.

Client Confidential

18. The AimJunkies *Destiny 2* cheat appears to interact with the *Destiny 2* game client in unauthorized and potentially dangerous ways.
19. The AimJunkies loader intentionally attempts to complicate debugging and reverse-engineering efforts and obfuscate loader operation through techniques commonly associated with malware. While the loader itself does not appear to be malware as traditionally understood, its presence and operation on a user's device represents a critical security vulnerability to that user.
20. The AimJunkies *Destiny 2* cheat provides cheaters with unfair competitive advantages against their fellow players in both competitive and cooperative gameplay. The continuing presence of cheaters in the game environment discourages communication between players and game developers, disincentivizes digital content creators from featuring the game, and drives legitimate current and prospective players away from the game entirely – all of which cause harm to Bungie.

Background & Opinions

Background

General Definitions and Categorization

21. On a broad level, a video game can be defined as “any of various interactive games played using a specialized electronic gaming device or a computer or mobile device and a television or other display screen, along with a means to control graphic images.”¹
22. In a more colloquial sense, a video game may be thought of as any form of interactive entertainment operated via technology – most commonly a personal computer, specific gaming console such as Sony's Playstation or Microsoft's Xbox, or through a smartphone. The interactive nature of the entertainment is what truly defines a video game. This interaction distinguishes video games from traditional entertainment forms such as film and music, which are absorbed more or less passively.
23. The video game industry in the United States has rapidly become the most profitable entertainment industry, far outstripping both the film, music, and professional sporting industries in terms of profit. Even in 1982, the arcade video game industry made \$8 billion, more than the revenues of pop music (\$4 billion) and Hollywood films (\$3 billion).² The industry has only grown since 1982; during 2020, the video game industry reported revenues surpassing the combined revenues of the film industry and North American professional sports.³ 73% of Americans reported playing a video game of some variety in 2021.⁴

¹<https://www.dictionary.com/browse/video-game>

²Rogers, Everett M.; Larsen, Judith K., *Silicon Valley Fever: Growth of High-technology Culture*, 1985.

³<https://www.marketwatch.com/story/videogames-are-a-bigger-industry-than-sports-and-movies-combined-thanks-to-the-pandemic-11608654990>

⁴<https://www.statista.com/statistics/499703/share-consumers-ever-play-video-games-by-age-usa/>, Vorhaus Digital Strategy Study 2022, p. 91

Client Confidential

24. The broad category of video games may be subdivided into a variety of genres. Genres are based on gameplay elements, settings, or basic structural models that follow accepted standards of gameplay and style. These genres themselves may be further subdivided into more specific categories. For the purposes of this report, only genres and categories that apply to Bungie's *Destiny 2* are defined here.
25. *Destiny 2* may be categorized as a "first-person shooter," a "massively multiplayer online" game, and a "looter-shooter."
26. In a "first-person shooter,"⁵ the player experiences the game environment from the first-person perspective, that is, through the eyes of their in-game character. Gameplay heavily features the use of virtual guns or other weapons as the primary method of play. Success within the game environment is defined by survival in simulated combat, either against computer-controlled enemies or against other players.
27. A "massively multiplayer online"⁶ (MMO) game is defined as "any online video game in which a player interacts with a large number of other players." MMOs generally require connection to a remote server for game operation. Social interactions and other community-driven features are often key components of an MMO game. Players may join together to form defined in-game groups, defined in *Destiny 2* as "clans." They find other players for cooperative or competitive play through "looking for group" and matchmaking features.
28. Based on their specific styles of gameplay, or the "gameplay loop," first-person shooter games may be then further subdivided into more specific categories. *Destiny 2* is termed a "looter-shooter." One of the primary goals of *Destiny 2* players is the acquisition of new in-game items, most commonly weapons and armor. Within the *Destiny 2* environment, such items are subject to randomization of various attributes that may dramatically increase the item's effectiveness or value to the player. As a result, the pursuit of these in-game items, also known as "loot," often by repeating activities over long periods of time, forms a core component of *Destiny 2* gameplay. The fact that "loot" is given to players as a reward for completion of gameplay objectives ("shooting"), is what defines *Destiny 2* as a "looter-shooter."
29. With these definitions in mind, *Destiny 2* may be described as a "first-person looter-shooter massively multiplayer online game." Players control their in-game characters from a first-person perspective while completing objectives, frequently based in combat, to gain loot, often with real-world friends or new social connections made during the course of *Destiny 2* gameplay. Players are given multiple options to compete against other players in player vs. player activities.

Genre- & *Destiny 2*-specific Terminology

30. While the above definitions and classifications may serve to give a broad overview of Bungie's *Destiny 2*, this report will make use of multiple genre-specific and game-specific terminology beyond the scope of the definitions above. These terms are defined below for clarity.

⁵<https://www.dictionary.com/browse/first-person-shooter>

⁶<https://www.dictionary.com/browse/mmo>

Client Confidential

31. MMO games such as *Destiny 2* provide features that may be broadly divided into two categories: “player vs. environment” or “PvE” activities, and “player vs. player,” or “PvP” activities. Players complete these activities using their “player character.”
32. A “player character” is the model through which the player interacts with the game world. In *Destiny 2* and its player community, a player character is also referred to as a “Guardian,” the term used within the narrative of the game to describe players. I will refer to player characters in *Destiny 2* as “Guardians.” An image from *Destiny 2* of a Guardian is shown below.



33. These player characters are distinct from “non-player characters,” or “NPCs.” The term NPC generally refers to any computer-controlled entity within a video game. Colloquially, NPCs more specifically refer to characters who interact with the player in some capacity. A NPC in a game may be an ally who assists the player, may assign the player activities, or may be an enemy of the player.
34. In “player vs. environment,” or “PvE” activities, players fight either individually or cooperatively against NPCs. The primary gameplay loops of *Destiny 2* may be classified as PvE activities.
35. In “player vs. player,” or “PvP” activities, players engage other players as opposed to NPCs. PvP activities may feature players competing to complete a specific goal – often point-based and defined in-game – or else engaging in direct competitive combat with one another. This variety of gameplay usually takes place as a “match” in some kind of in-game arena and involves shooting the Guardians of other players to do “damage,” a value defined by the gun a character is shooting and the player’s accuracy. Once a player has been dealt a certain amount of damage, they are defeated and removed from the arena. Defeating another player typically awards points. *Destiny 2* offers PvP activities for both 6 and 12 players at a time, split into equal teams.
36. The use of the term “map” in the context of this report should be understood to refer to the 3D landscape used as the setting for a game’s action. In a PvP match, the map refers to the entire arena used for that match. For example, “from across the map” typically refers to an action that has occurred across a substantial distance. The ability to “see through the map” refers to the power to see through walls or other obstacles that would typically block a player’s line of sight. This is the advantage provided by the AimJunkies *Destiny 2* cheat.

Client Confidential

37. As players use the in-game weapons of a video game, they frequently have the ability to better aim their weapon by using that weapon's simulated sights. This ability, known as "aim-down-sights," or "ADS," refers to a player zooming in with their weapon as though looking down weapon sights or a scope. The camera will zoom in to provide a larger target and afford a player increased weapon accuracy. Examples of views showing a weapon without ADS (on the left) and with ADS (on the right) are shown below.



38. One of the most common features of first-person shooter games such as *Destiny 2* is the inclusion of a common weak spot on enemies encountered by the player. (These weak spots are assigned not just to NPCs, but to the Guardians of other players during PvP activities as well.) As this weak spot is generally a target's head, a critical hit on such a spot is commonly referred to as a "headshot" by players, even if this weak spot is located elsewhere on an enemy's body. Within *Destiny 2*, some in-game weapons are capable of defeating an opposing player in a PvP match with a single headshot.
39. A "heads-up display," or "HUD," refers to graphical elements within the game that provide information to the player. A HUD typically includes information about a player's current health, equipped weapons and remaining ammunition, an overview of their current ability status, or any other data deemed relevant by the developers of the game.
40. The HUD of a *Destiny 2* player also includes a "radar," a graphical element that grants a player information about the locations of other Guardians or NPC enemies, even if the player cannot directly see them. The radar available to players in *Destiny 2* does not provide the exact locations of other players or NPCs, but rather their general direction and distance relative to the player's Guardian. A screenshot showing the standard HUD from *Destiny 2* is shown below, with circles drawn around some of the elements described in paragraphs 38-39.

Client Confidential

Game Devices and Digital Download

41. Modern video game players have a wide variety of options when choosing a technological method, or “platform,” on which to play their games. Platforms fall into three broad categories: personal computers (“PCs”); dedicated game consoles (“consoles”); and mobile devices. Bungie’s *Destiny 2* is available to players on PCs and consoles.
42. In this report, a PC refers to a desktop or laptop computer running the Windows operating system. As there are significant structural differences between the Windows operating system published by Microsoft, the macOS published by Apple for their Mac computers, and versions of the open-source Linux operating system, Mac and Linux computers are commonly considered a separate category from Windows-based PCs. For the purposes of this report, the term PC should be understood as a personal computer running the Windows operating system.
43. Consoles may be defined as “computer systems specially made for playing video games that are connected to televisions or other displays for video and sound.”⁷ Consoles are purpose-built in order to provide players with a computer powerful enough to run modern games easily. Consoles generally feature an operating system unique to that family of devices, allowing software to be optimized by a variety of developers. Commonly owned consoles include Microsoft’s Xbox, Sony’s Playstation, Nintendo’s Switch, or Google’s Stadia. *Destiny 2* is available on the Xbox and Playstation.
44. The vast majority of modern games are delivered to consumers via digital download; many games no longer offer any hardware-based (i.e., CD-ROM or DVD) installation mechanism. As of 2013, digital downloads accounted for more than half of all video games sold; as of 2018, over

⁷<https://www.dictionary.com/browse/game-console>

Client Confidential

80% of purchased games were provided to customers via digital download.⁸ Files required for game operation are downloaded and stored directly on a consumer's device, allowing for faster updates from developers, clearer communication between devices and game servers, and lower costs for developers. Purchases for these digital downloads are handled through a variety of marketplace services, depending on the platform.

Technical Terms

45. While full definitions of every technical aspect of video games and client/server interactions are beyond the scope of this report, I will refer to several key concepts which are briefly defined as follows.
46. An "instance" is a "zone to which access is limited to a player or group of players entering simultaneously and working together. Each instance is one copy of the zone in which the quests, enemies, items, events, etc are staged exclusively for the player or group accessing it, without interference from other player characters in the large online population of the game."⁹ For example, when players compete in PvP matches against one another, they may be said to be "within an instance." Players may not randomly join the match, and the instance's isolation prevents players not involved in the match from influencing it.
47. The "game client," or, simply, the "client," refers to the locally stored and executed version of a game used by players to interact with the game world. In the case of Bungie's *Destiny 2* (and the overwhelming majority of modern video games), the client is digitally downloaded and stored on a user's file system until loaded into memory for use.
48. "Game servers," or, simply, "servers," refer to the specialized networking devices used by the game developers to connect players to shared, multiplayer instances facilitated by their game client. Servers provide information about the environment to players. Each game client reports the player's actions to the server, and the server updates all players with the results of those actions.
49. The "game state" refers to the positions and statuses of all game pieces and environmental features at any given time. In *Destiny 2*, the positions of each player, their velocity and trajectory, the direction they are facing, and their health are just some of the elements that comprise the game state. The server coordinates changes to the game state and communicates those changes to a player's client.
50. The protocols used by clients and servers to update and communicate this game state data may collectively be referred to as "netcode." This includes procedures for reconciling differences in game state as reported by different clients. Colloquially, players use "netcode" as an umbrella term for the overall consistency and responsiveness of the gameplay experience while playing online.

⁸<https://www.statista.com/statistics/190225/digital-and-physical-game-sales-in-the-us-since-2009/>

⁹<https://www.dictionary.com/browse/instance>

Client Confidential

Importance of Viral Marketing

51. The use of social media for advertising and marketing represents one of the fastest-growing and most powerful tools available to companies. The International Trade Administration of the U.S. Department of Commerce forecast a growth rate of 18.1% per year through 2026 for the global social media advertising segment.¹⁰
52. Recognizing its value, Bungie makes extensive first-party use of social media and viral marketing to promote *Destiny 2*. Reliance on social media and viral marketing is a widespread industry practice, but Bungie makes particularly effective use of these outlets. While Bungie maintains a footprint on all major social media platforms, including Facebook¹¹ and Instagram,¹² their strongest presence appears on Twitter and Reddit. On Twitter alone, Bungie operates a corporate account,¹³ a *Destiny 2*-specific account,¹⁴ and a third account solely for providing technical updates and support for the *Destiny* game environments.¹⁵
53. In addition to these first-party accounts, Bungie employs specific personnel known as Community Managers¹⁶ to interact with the *Destiny* community through repurposed personal accounts. These Community Managers write blog posts distributed through social media, respond to community concerns and statements, and generally act as liaisons between game developers and the fans of their game.
54. This kind of first-party social media marketing allows Bungie and other companies like it to interact directly with and promote content creators, influencers, and other members of their gaming communities. These interactions in turn provide players with a feeling of ownership and personal investment in the game, allowing them to feel seen by the developers, including Bungie, in a way unique to social media marketing.
55. Content creators and influencers who find satisfaction in these interactions provide immeasurable value to companies by continuing to produce content about the game. This content keeps discussion of the game in the public eye, recruits new players, encourages lapsed users to resume playing, and creates further connections to the game for active players through deepened interactions with these streamers. The most influential streamers for *Destiny 2* list over one million YouTube or Twitch.tv subscribers. Particularly popular videos or content may have an even broader reach.
56. While no concrete metrics exist to evaluate the value of such marketing, Bungie very clearly displays a great deal of skill and interest in promoting these creators and in fostering an active streamer community. A perfect example of this may be seen in Bungie's biannual World First Day One Race event,¹⁷ in which a new six-player activity known as a "raid" is released into the game for the first time. The first team of six players to complete this activity within the first 24 hours of

¹⁰<https://www.trade.gov/ecommerce-frontline-social-media-forecast>

¹¹<https://www.facebook.com/Bungie/>

¹²<https://www.instagram.com/bungie/?hl=en>

¹³<https://twitter.com/Bungie>, 2.8 million followers

¹⁴<https://twitter.com/DestinyTheGame>, 2.7 million followers

¹⁵<https://twitter.com/BungieHelp>, 1 million followers

¹⁶<https://www.indeed.com/hire/job-description/community-manager>

¹⁷<https://www.youtube.com/watch?v=WiAd15wfVRo>

Client Confidential

release is promoted heavily by Bungie through their social media arms. The winning team receives a variety of physical prizes, and other players who achieve a Day One completion can earn coveted in-game rewards.

57. The success of this positive feedback loop between developers, fans, and content creators over social media is contingent upon the health of the game environment and positive player feelings toward the game. Strong player feedback and a tightly-knit community encourage content creators to continue promoting the game, which in turn encourages developers to take a more active role in community engagement and involvement. This creates a sense of positive ownership for fans, and the cycle continues. When negative third-party elements invade this space – when players encounter cheaters acting independently of the game developers, for example – the well is poisoned, and the feedback loop degrades. Angry fans are less likely to play the game, and developers are less likely to interact with the increasingly negative feedback. Interest in game content diminishes, and content creators feel less incentive to continue. All of this harms Bungie’s brand and reputation.

Game Ecosystem Investment

Game Setting and Suspension of Disbelief

58. While video games are by definition an interactive experience, they share many of the same conceits and structural concerns as other narratives. The effectiveness of the game turns on the concept of suspension of disbelief, “the concept that to become emotionally involved in a narrative, audiences must react as if the characters are real and the events are happening now, even though they know it is ‘only a story.’”¹⁸ Films, literature, and art rely upon this suspension of disbelief to engage consumers. Viewers who feel the world is real and alive are much more likely to remain invested. Successfully evoking suspension of disbelief is the sign of a compelling narrative or idea that consumers will continue to seek out.
59. In the interactive medium of a video game, the suspension of disbelief takes on an even greater importance for developers. Players who feel as if they are part of a dynamic world in which they have agency tend to invest more money and time in the game.
60. Video game developers therefore take pains to design and implement varied and detailed environments within the game in an effort to enhance the suspension of disbelief. These environments are often woven into the game’s larger narrative in ways that resemble classical literary techniques in order to strengthen the perception that the player is part of a living world in which their choices carry weight.
61. To this end, video games may be set in nearly any genre or variety of location. *Destiny 2*, a work of science fiction, takes place centuries in the future in various locations across the solar system. Players are pitted against extraterrestrial enemies in the corridors of space ships, the ruins of Earth cities, or on an icy moon of Jupiter. *Destiny 2* Guardians, created by players as their in-game avatars, are immortal warriors of peerless combat prowess.

¹⁸<https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100544310>

Client Confidential**Long Term Player Investment**

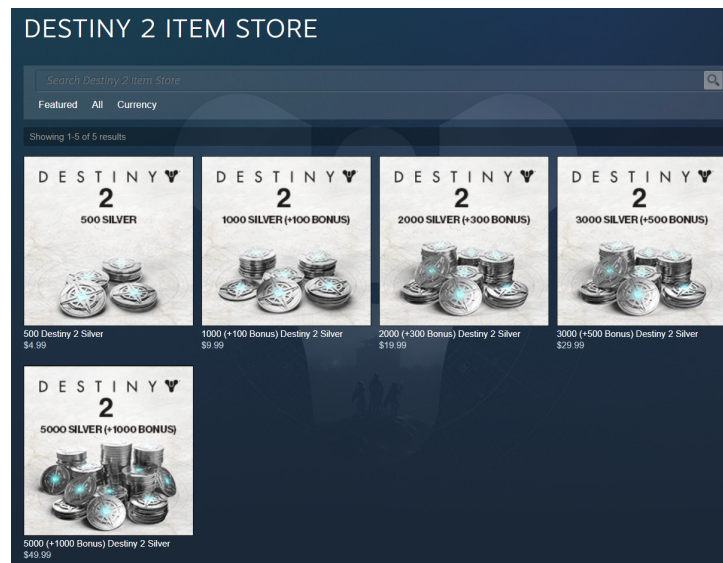
62. Suspension of disbelief through compelling narrative and well-designed environments is a useful tool for solidifying a player's emotional and financial investment. Yet while positive investment during a game's release cycle can build early awareness and consumer excitement about future property, this excitement will only last so long without additional investment. Players and video game media outlets quickly move to the next offering as the initial excitement fades.
63. The issue of long-term investment is increasingly addressed by adopting a responsive software-as-a-service model (SaaS), particularly by developers of MMO games like *Destiny 2*.
64. Games designed using this model are considered to be "living games." Very few elements are wholly static. Instead, they may be updated, expanded on, or removed by game developers for a variety of reasons. SaaS games receive frequent updates, or "patches," from developers. These may increase the game's stability or change its mechanics, improvements frequently referred to as "balancing." For example, the amount of damage a gun does to an enemy may be reduced or increased based on gameplay performance. The health of an enemy may be increased to add difficulty to the game experience. Bugs within the game may be resolved to increase the game's general stability.
65. The most basic versions of many SaaS games, including *Destiny 2*, are increasingly offered to consumers for free in an effort to draw in new customers. Known as "free-to-play" (FtP), this model allows players access to basic features or to an introductory storyline of a game in the hope that the player, after experiencing the game's core offering, will pay for additional content.
66. Additional content not included with the original or "base" version of a game may be offered at any point within the game's life cycle. Some of this content may be offered as free additions, but additional content more commonly requires a user purchase. Large expansions to the game's mechanics, items, and environments may be offered to players as "expansion packs" or "downloadable content" (DLC). The prices for this content vary depending on the developer and level of change to the game itself.
67. *Destiny 2* is free to play, but offers multiple content expansion packs to players for purchase. While the new features of a paid expansion may only be available to players that have purchased the upgrade, they do not usually offer a competitive advantage, or do so only in carefully considered ways. The reasoning for this is explained below in the "Competition and Fairness" section of this report.
68. FtP and SaaS model games generally employ release cycles of varying lengths for regular content upgrades, referred to as a "seasonal model." Large changes and updates are made on a regular schedule to encourage players to come back to the game over longer intervals. *Destiny 2* uses a seasonal model, with content typically refreshed within the game every three months, and individual narrative story "beats" released on a week-by-week basis.
69. In a *Destiny 2* season, players are delivered a new narrative experience, multiple new activities, new items to earn, and, typically, an expansion of features or functionality. This cycle is designed to encourage a positive, shared narrative experience for all active players, to encourage players to continue or resume play, and potentially to spend more money at more frequent intervals. As

Client Confidential

with the content expansion packages, these features do not generally offer competitive advantages to the players who purchase them.

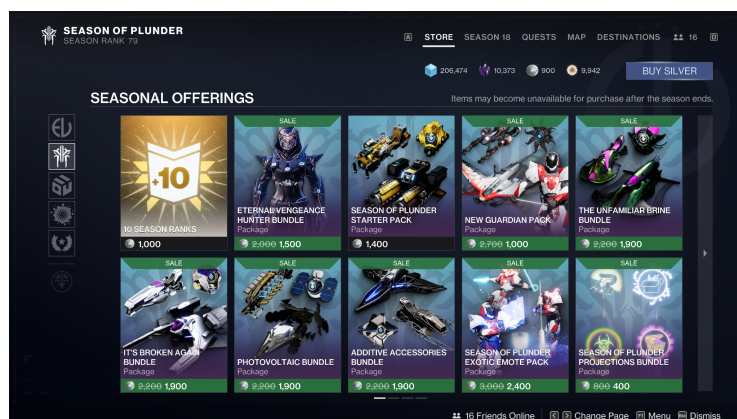
Microtransactions and Cosmetic Purchases

70. In addition to the release of DLC and seasonal content, *Destiny 2* also offers players an in-game store where, for additional cost, players may purchase cosmetic changes (“cosmetics” or “ornaments”) for their characters’ armor, weapons, tools, and vehicles. Each ornament is offered for a low one-time cost to players, a business model known as “microtransactions.”¹⁹ The concept of this business model is clear; rather than relying on new sales of the game, players are given further opportunities to spend incremental amounts within the game they already own whenever they like.
71. Almost universally, these microtransactions are made within the game environment itself with a “premium currency” separate from the usual items and currencies of the game. While this currency may be earned in-game in some cases, its premium status derives from its ability to be purchased with real-world money. Cosmetic microtransactions within the game are listed in this currency, which may be purchased by players in packs of varying sizes and prices. Discounts are generally offered to players who purchase more premium currency in a single transaction.
72. Bungie’s *Destiny 2* uses the premium currency “Reef Silver,” or, simply, “Silver.” Within *Destiny 2*, Silver is only obtainable by purchasing packs of the currency from the relevant platform store. For example, on the Steam platform for PC, *Destiny 2* has the following Silver packs available for player purchase:



73. After purchasing one of these packs, the amount immediately becomes available in that player’s in-game account balance. As seen in the image below, taken from the in-game *Destiny 2* store, the premium currency can be redeemed in-game to obtain levels, cosmetic ornaments, or other player items or attributes.

¹⁹<https://www.jstor.org/stable/j.ctv1hp5hqw.13>

Client Confidential

74. Players within *Destiny 2* are offered a variety of cosmetic microtransactions for purchase, with new cosmetics being added to the in-game store on a regular basis. These cosmetic offerings encourage players to routinely purchase bundles of the in-game premium currency and provide the developers a consistent revenue stream beyond the initial release of a game, which in turn funds the continued development of compelling content that encourages players to invest more deeply in the game. Players who make these purchases tend to be more loyal to the game, to feel pride and a sense of ownership over their well-appointed avatar, and to have a continued desire to engage with the game's ongoing narrative and the community of other players.

Security Relationships

75. In multiplayer games that offer competitive play against other players (PvP play), video game developers have a clear interest in promoting fairness within the game.
76. In the context of PvP play, fairness may be thought of as supplying a level starting position for all players. No player should be seen to have an immediate advantage over another because they have spent more money. Such games develop a reputation as “pay-to-win” games, where players who have spent more real-world money have an overwhelming advantage over those who have not. In *Destiny 2*, select abilities and exotic weapons are locked behind purchase of expansions, but their efficacy is balanced to avoid creating a “pay-to-win” environment.
77. Competitive games strive to avoid a “pay-to-win” impression, as these games tend to drive players away from the game environment. Only a small subset of players will have resources to buy every upgrade, meaning that the average player competing against them will always be at a disadvantage.²⁰ In a race between a high performance sports car and a family minivan, the sports car clearly has every advantage over the minivan, and will almost certainly win the race. Why would the driver of the minivan agree to the race in the first place? This is why developers are careful not to include goods that confer competitive advantages in upgrade packages.
78. Game developers have a clear incentive then to provide each player within a multiplayer environment a level playing field independent of that player's financial commitment. There is an

²⁰<https://kotaku.com/diablo-immortal-p2w-pvp-broken-blizzard-rite-exile-1849355846>, titled: “Diablo Immortal Player Says He Can’t Get A Match After Spending \$100,000.”

Client Confidential

implicit understanding between developer and player that the developer will create, promote, and maintain the idea that a player's skill is what defines their competitive success, not the money they have paid.

79. Competitive video games, including *Destiny 2*, enforce this principle in the agreements each user must sign, typically referred to as an end-user license agreement (EULA), limited software license agreement (LSLA), or terms of service (ToS). The *Destiny 2* LSLA itself states that users may not "hack or modify the Program, or create, develop, modify, distribute, or use any unauthorized software programs to gain advantage in any online or multiplayer game modes."²¹ The user purchases a license to install and use one copy of the game software and only as installed by the game software or platform itself. Users are not permitted to manipulate (e.g., copy, reverse engineer, or commercially exploit) the *Destiny 2* software. Specific enumerated "LICENSE CONDITIONS" in the LSLA and EULA, if violated, result in immediate termination of the license; and users are warned that continued use of the program "will be an infringement of Bungie's copyrights in and to the Program." *Id.* The document further notes that violation of any of its clauses entitles Bungie to suspend or ban the account found to be in violation of the ToS, and to take any further remedies available and deemed appropriate. The EULA, which tracks to the LSLA, is displayed prominently when a user runs the *Destiny 2* software for the first time and on each occasion that the EULA is changed. The user is required to indicate assent by holding a controller, keyboard, or mouse command.

Cheating in Video Games

80. "AimJunkies" is a cheat software brand and the domain name for a website from which the cheat software is sold. Cheats for live-service online multiplayer games like *Destiny 2* are developed by third-party actors like AimJunkies' owner Phoenix Digital Group LLC (PDG), who profit by offering video game users unfair and unauthorized advantages. "AimJunkies" will be used throughout to refer to the owners of PDG and to the network of developers who create cheat software to be sold under the AimJunkies brand.
81. Video game companies protect their games to prevent manipulation and copying of their software, and they advertise the fact that these protections are in place. AimJunkies and other cheat developers circumvent these protection measures, and are advertised as circumventing these protections, to introduce features not foreseen by the games' developers that degrade the game as a whole.
82. Customers are almost always charged for cheats for live-service online multiplayer games, and cheat developers often require a monetary subscription to their provider for continued functionality.
83. Cheats for live-service online multiplayer games are frequently intended for use within a shared online environment with potentially thousands of other players.
84. Cheats for live-service online multiplayer games are frequently advertised using highlight videos of the cheat in action against unsuspecting players of the game.

²¹<https://www.bungie.net/7/en/legal/sla>

Client Confidential

85. Cheats for live-service online multiplayer games, including the AimJunkies cheat, typically require users to disable system security protections. Since the cheat must inject itself into low-level system processes to circumvent *Destiny 2*'s anti-cheat measures, both native and third-party antivirus software frequently block the cheat from download or installation. Almost universally, cheat installation instructions instruct users not just to disable, but to remove entirely any installed antivirus software from their computer. Native features such as Microsoft's Windows Defender must be disabled from an administrator account. All firewalls must be uninstalled and removed entirely, or else disabled from an administrator account. Users must enter their computer's BIOS, the most basic and essential firmware typically packaged with their motherboard, and disable key stability and security features. These protections are there to prevent malicious programs from accessing core operating system components of the user's computer that can be used to take it over. Software installation does not normally require the disabling or removal of such protections. When users disable these protections in order to install the cheat, they render their computers susceptible to viruses, trojans, and ransomware. If a cheat developer decides to use this access for their own ends, consumers no longer have standard protections in place to defend against this.
86. As a result, modern cheats are frequently flagged by antivirus software and threat intelligence vendors as malware. While the cheat itself may not execute ransomware or steal a user's data, simply installing it according to the cheat developer's instructions opens the user's computer to the possibility of immediate and catastrophic attack.

The Anatomy of a Modern Cheat

Relevant Terminology

87. The success of modern cheats is a function of the quality and quantity of features they offer potential customers. Often, these features are described with slang, jargon, and acronyms that do not provide any information about how they actually work. Some cheat features and their functionality are described below.
88. One of the most common features sold by cheat developers is the classic "aimbot." This cheat functionality automates the movements of a player's Guardian as they attempt to aim their weapon at a specific target. An aimbot is typically configured to snap to an opponent's head when the player goes into ADS. The cheat confers perfect accuracy on the Guardian, giving them the ability to score headshots with every shot to rapidly eliminate opponents.
89. A wide range of cheat functionality may be defined under the category "extrasensory perception," or "ESP." ESP functionalities provide data to the cheating player about the game state that would normally be hidden to them, such as the locations of other players behind walls, the state of another player's health, or the status of their abilities.
90. The most common ESP feature built into modern cheats is the "wallhack," the ability to see through opaque objects such as walls. Cheats will typically highlight another player's Guardian's exact location when line-of-sight is obstructed. Wallhack is also used as a generic slang term for the ability to see through the map. While some games, including *Destiny 2*, grant this ability to

Client Confidential

players under certain constraints, a cheat wallhack grants this information without the conditions, limitations, or structures imposed by the game's developers.

91. The image below, taken from an AimJunkies promotional video for their *Destiny 2* cheat, demonstrates this functionality well.²² In the image below, although the NPC enemies should be obscured from the view of the player by pillars and other objects, the AimJunkies cheat identifies them by highlighting their locations using yellow boxes.



92. With these definitions in mind, a general description of the technical operations of the AimJunkies cheat may be provided. This description must begin with several caveats, however.
93. I have personally participated in the acquisition, review, and analysis of multiple cheats for *Destiny 2* throughout the course of my work. This includes de-compilation, or unpacking, of cheat executables for code analysis and potential reverse-engineering.
94. While I have examined other cheats for *Destiny 2*, it does not at present appear to be possible to directly examine the specific *Destiny 2* cheat produced and sold by AimJunkies. My understanding is that the Respondents in this arbitration have not produced a copy of the cheat.
95. However, I have conducted static and dynamic analysis of the currently available AimJunkies cheat loader. I have further reviewed and analyzed footage of the AimJunkies *Destiny 2* cheat in operation in promotional videos that I understand were captured and archived for the purpose of this arbitration.
96. Even absent the *Destiny 2* specific cheat files, I have been able to draw reasonable inferences about the AimJunkies *Destiny 2* cheat through these analyses, review of accessible footage of the cheat in operation, and the similarity of the AimJunkies loader and framework to comparable cheats.

²² BUNGIE_WDWA_0000469

Client Confidential

AimJunkies Cheat Loader Download and Installation

97. Cheats for *Destiny 2* are distributed by means of a specialized program called a “loader.” The loader is a program that authenticates the cheat user, validates their purchased license, downloads the cheat itself, and injects that cheat into Microsoft Windows system libraries and/or into the game client module.
98. For the AimJunkies *Destiny 2* cheat, this loader is first downloaded by a user immediately after the purchase of a cheat from the AimJunkies website. The loader represents a serious threat to users who follow AimJunkies’ instructions.
99. After purchasing an AimJunkies cheat and downloading the loader, AimJunkies provides the cheat user a how-to guide²³ for installation through their forums. These instructions direct the user to perform several highly unsafe actions on their PC. Samples of these instructions were taken from the AimJunkies website in early September 2022 and are provided in the following paragraphs.
100. The process described in these instructions is potentially highly dangerous to the user, as it involves disabling or creating exceptions in antivirus and firewall services, disabling Windows security controls, and granting the loader full administrative rights to the user’s device. Users following these instructions potentially open themselves to ransomware, data theft or loss, and other forms of cyberattack.
101. In their installation instructions, AimJunkies recommends that users upgrade their Windows operating system to the latest version. On its face, this is a reasonable step before installing any software. However, in heading-size font, AimJunkies immediately notes that two Microsoft patches, KB5014666 and KB5015807, “can cause problems with the cheats.”^{24,25} The instructions recommend that users uninstall these patches. Since Microsoft’s published patch notes describe KB5015807 as a “security update,” and both patches appear to introduce security and quality of life improvements to the Windows operating system, this recommendation raises security questions.

NOTE: It is a know that the following MS patch KBs can cause problems with the cheats. If you have KB5014666 & KB5015807 installed, please uninstall them

102. The loader installation instructions further direct the user to install and “place the loader on a USB Flash drive formatted in FAT32 (This is a security measure).” This is false. Selecting FAT32 as the file system does not impart any security features to the newly formatted drive. Instead, placing the loader on this fresh drive serves to prevent the loader from being immediately quarantined by system antivirus measures.
103. Users are next instructed to add an exception to the Windows Defender antivirus and security tool which comes packaged with all current Windows operating systems. Windows itself strongly

²³[https://forum.aimjunkies\[.\]com/f139/read-thread-just-bought-cheat-134981/](https://forum.aimjunkies[.]com/f139/read-thread-just-bought-cheat-134981/)

²⁴<https://support.microsoft.com/en-us/topic/june-28-2022-kb5014666-os-builds-19042-1806-19043-1806-and-19044-1806-preview-4bd911df-f290-4753-bdec-a83bc8709eb6>

²⁵<https://support.microsoft.com/en-us/topic/july-12-2022-kb5015807-os-builds-19042-1826-19043-1826-and-19044-1826-8c8ea8fe-ec83-467d-86fb-a2f48a85eb41>

Client Confidential

advises against disabling Defender entirely; even less technically adept cheat purchasers would be likely to recognize disabling Defender as a dangerous step. Adding an exception for AimJunkies allows users to feel they are still protected, but this “precaution” is no less dangerous than simply turning the antivirus protection off. This step marks any files within the AimJunkies installation folder as trusted, meaning any process execution originating from this folder will be ignored by Windows Defender. Coupled with further AimJunkies installation steps, this represents a critical vulnerability to users.

Windows Defender – Add the Exception ****DO NOT DISABLE**

- Open Windows Defender by searching for "Windows Security" in the start menu and clicking on the result.
- Click on the "Virus & Threat Protection" option.
- The above action will take you to the Virus & Threat Protection screen. Here, click on the "Manage Settings" link under Virus & Threat Protection Settings section.
- In the advanced options page, scroll down until you find the Exclusions section. Here, click on the "Add or remove exclusions" link.
- This is where you can add exclusions. To exclude a folder, click on the "Add an exclusion" button and then select the "Folder" option.
- The above action will open the "Browse" window. Find the folder you want to exclude, select it, and click on the "Select Folder" button. I would recommend exclude the folder to where the loader will download into as well as the entire drive letter of the USB flash drive you put your loader onto.
- Close the application.

104. Users are further directed to add an exception within the Windows Firewall configuration, also packaged with all current Windows operating systems. As before, the exception allows users to feel they are still protected, but this exception is again as dangerous as simply turning the firewall off.
105. AimJunkies' users are directed to disable the User Account Control (UAC)²⁶ features also packaged with all current Windows operating systems. UAC features prompt the user for confirmation before any major changes may be made to the settings, configurations, or installed applications of an operating system. As a result, UAC features function as a strong defense against malware infection. Disabling UAC allows any program, such as the AimJunkies *Destiny 2* cheat, to make administrative changes to the device – and to do it without the user's knowledge.

Disable UAC

- Go to Control Panel and go to "User Accounts".
- Go to User Accounts.
- Change User Account Control Settings, move the slider all the way to the bottom and click "Ok" to apply this setting.

106. In the final step of the loader installation instructions, AimJunkies provides a note about third-party software that says, "AimJunkies only supports using Windows Defender/Firewall." Since what the user has actually done is manually created exceptions for the AimJunkies loader through these services, a more accurate statement would be, "AimJunkies only provides instructions for evading Windows Defender/Firewall." AimJunkies then provides a list of

²⁶<https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/how-user-account-control-works>

Client Confidential

third-party security software that “have caused known issues with our loader/cheat, please disable or uninstall them if you run into issues using the loader/cheat.” This list includes several major security software vendors as well as anti-cheat software used by game developers.

*****A Note About 3rd Party Software*****

While our loader/cheats may work with other 3rd party security programs, however AimJunkies only supports using Windows Defender/Firewall.

The following have caused known issues with our loader/cheat, please disable or uninstall them if you run into issues using the loader/cheat.

- Riot Vanguard
- Malwarebytes
- QQ Protect
- F-PROT
- AlibabaProtect
- AVAST
- ESET
- Norton/Symantec
- Kapersky
- Bit Defender
- AVG
- McAfee
- IO Bit
- Warsaw and/or GAS Technologies
- Notepad++
- ASUS Armory Crate
- ASUS AI Suite
- WebRoot
- Wallpaper Engine 32
- Various Avira
- Razer Cortex
- Various Avira
- MSI Afterburner
- Any VmWare or Virtual Machine software

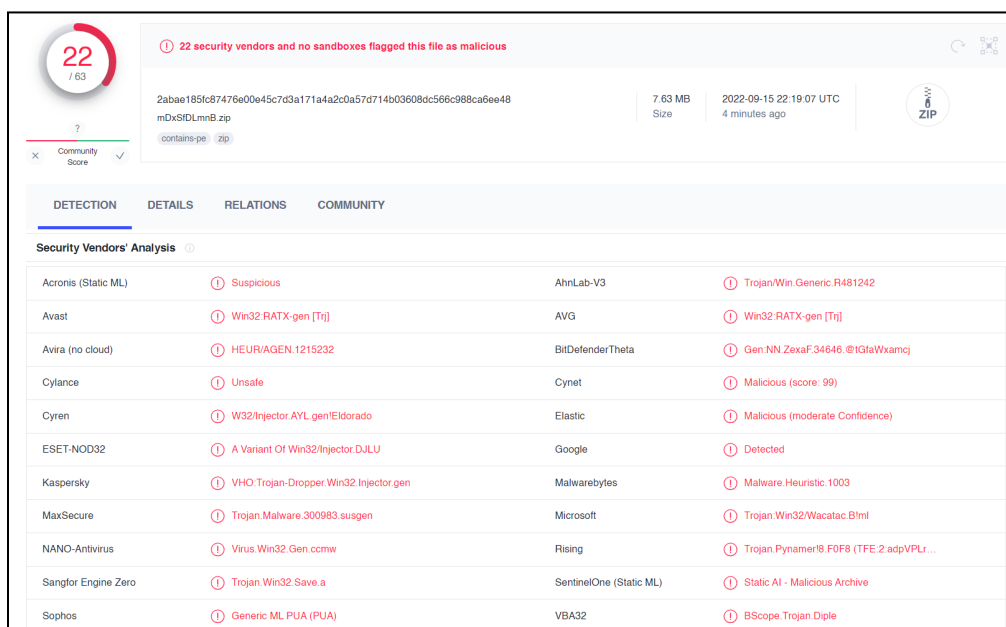
AimJunkies Cheat Loader: Static Analysis

107. On September 15, 2022, I performed static analysis on the AimJunkies cheat loader. I acquired the loader from their website as a compressed .zip archive and used the industry standard malware analysis platform VirusTotal for the analysis.²⁷ The archive contains two files: a .cfg configuration file used to define settings and other variables for installation, and a .exe portable executable file, which appears to be the AimJunkies loader itself. The archive in its compressed form and the two files it contains were each analyzed independently. Note that this loader is not the same thing as the cheat software specific to *Destiny 2*. The loader’s function is to facilitate the operation of game-specific cheat software modules like the *Destiny 2* cheat on a user’s computer.
108. Static malware analysis examines suspect resources – in this case, the .zip archive, the .exe, and the .cfg configuration file – in their at-rest state. The programs are not executed or installed. Information about the general behavior and characteristics of the file may be gathered with this analysis. Code decompilation reveals some data about functionality and system interaction.

²⁷<https://www.virustotal.com/>

Client Confidential

109. Dynamic malware analysis involves executing the suspect resource and observing the resulting behavior. Dynamic malware analysis is typically conducted using debugging, monitoring, and logging tools to monitor system-wide effects of any executed malware.
110. One of the major strengths of the VirusTotal platform is its aggregation of analysis and assessments of potential threats from a wide range of vendors, including Microsoft, Google, Malwarebytes, Bitdefender, and many others. This aggregation helps avoid false positives potentially given by a single service or tool, and provides a more comprehensive understanding of the potential threats posed by an inspected resource.
111. As the list below shows, the compressed .zip archive used to download the loader from the AimJunkies website is flagged as potential malware by 22 vendors.²⁸



Security Vendors' Analysis			
Acronis (Static ML)	ⓘ Suspicious	AhnLab-V3	ⓘ Trojan.Win.Generic.R481242
Avast	ⓘ Win32:RATX-gen [Trj]	AVG	ⓘ Win32:RATX-gen [Trj]
Avira (no cloud)	ⓘ HEUR/AGEN.1215232	BitDefenderTheta	ⓘ Gen:NN.ZexaF.34646.@IGtaWxamcj
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 99)
Cyren	ⓘ W32/Injector.AYL.gen/Eldorado	Elastic	ⓘ Malicious (moderate Confidence)
ESET-NOD32	ⓘ A Variant Of Win32/Injector.DJLU	Google	ⓘ Detected
Kaspersky	ⓘ VHO:Trojan-Dropper.Win32.Injector.gen	Malwarebytes	ⓘ Malware.Heuristic.1003
MaxSecure	ⓘ Trojan.Malware.300983.susgen	Microsoft	ⓘ Trojan.Win32/Wacatac.B!ml
NANO-Antivirus	ⓘ Virus.Win32.Gen.ccmw	Rising	ⓘ Trojan.Pynamer%F0F8 (TFE.2.adpVPLr...
Sangfor Engine Zero	ⓘ Trojan.Win32.Save.a	SentinelOne (Static ML)	ⓘ Static AI - Malicious Archive
Sophos	ⓘ Generic.ML.PUA (PUA)	VBA32	ⓘ BScope.Trojan.Diple

112. The AimJunkies loader executable stored within this archive is flagged as potential malware by 48 vendors.²⁹ This number has increased from 31 since the loader was first uploaded to VirusTotal on September 15, 2022.

²⁸ <https://www.virustotal.com/gui/file/2abae185fc87476e00e45c7d3a171a4a2c0a57d714b03608dc566c988ca6ee48/detection>

²⁹ <https://www.virustotal.com/gui/file/f2c08cec764e85a42888250cf79747c47b3a7614199f2b4cba98b8745bb7749c/detection>

Client Confidential

48 / 70

48 security vendors and no sandboxes flagged this file as malicious

f2c08cec764e85a42888250cf79747c47b3a7614199f2b4cba98b8745bb7749c

7.65 MB Size

2022-09-17 17:49:00 UTC 2 months ago

wfDaEuMgRU.exe

peexe spreader upx

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY

Security vendors' analysis on 2022-09-17T17:49:00 UTC

Acronis (Static ML)	ⓘ Suspicious	Ad-Aware	ⓘ Trojan.GenericKD.62095134
AhnLab-V3	ⓘ Trojan.Win.Generic.R481242	Alibaba	ⓘ Trojan.Win32/Injector.415ca068
ALYac	ⓘ Gen.Variant.Fragtor.141921	Antiy-AVL	ⓘ Trojan.Generic.ASMalwS.51F4
Avast	ⓘ Win32-RATX-gen [Trj]	AVG	ⓘ Win32-RATX-gen [Trj]
Avira (no cloud)	ⓘ HEUR/AGEN.1215232	BitDefender	ⓘ Trojan.GenericKD.62095134
BitDefenderTheta	ⓘ Gen.NN.ZexaF.34646.@tGfaWxamcj	Bkav Pro	ⓘ W32.AIDetect.malware1
CrowdStrike Falcon	ⓘ Win/malicious_confidence_90% (W)	Cybereason	ⓘ Malicious.51c942
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 100)
Cyren	ⓘ W32/Injector.AYL.genIEldorado	Elastic	ⓘ Malicious (moderate Confidence)
Emsisoft	ⓘ Trojan.GenericKD.62095134 (B)	eScan	ⓘ Trojan.GenericKD.62095134
ESET-NOD32	ⓘ A Variant Of Win32/Injector.DJLU	Fortinet	ⓘ W32/DJLU/tr
GData	ⓘ Win32.Trojan.Agent.OHLA08	Google	ⓘ Detected
Gridinsoft (no cloud)	ⓘ Trojan.Heur!032120A9	Kaspersky	ⓘ Trojan.Win32.Inject.aokaf
Lionic	ⓘ Heuristic.File.Generic.00x1p	Malwarebytes	ⓘ Malware.Heuristic.1003
MAX	ⓘ Malware (ai Score=80)	MaxSecure	ⓘ Trojan.Malware.300983.susgen
McAfee	ⓘ Artemis!0D6FA42912BC	McAfee-GW-Edition	ⓘ BehavesLike.Win32.Generic.wc
Microsoft	ⓘ Trojan.Win32/Sabsik.FL.B!ml	NANO-Antivirus	ⓘ Virus.Win32.Gen.ccmw
Palo Alto Networks	ⓘ Generic.ml	QuickHeal	ⓘ TrojanDropper.Injector
Rising	ⓘ Trojan.Pynamer!8.F0F8 (CLOUD)	Sangfor Engine Zero	ⓘ Trojan.Win32.Save.a
SecureAge	ⓘ Malicious	SentinelOne (Static ML)	ⓘ Static AI - Malicious PE
Sophos	ⓘ Mal/Generic-S	Symantec	ⓘ ML.Attribute.HighConfidence
TEHTRIS	ⓘ Generic.Malware	Trapmine	ⓘ Malicious.high.ml.score
Trellix (FireEye)	ⓘ Generic.mg.0d6fa42912bc140f	TrendMicro-HouseCall	ⓘ TROJ_GEN.R002H0CIF22
VBA32	ⓘ BScope.Trojan.Diple	VIPRE	ⓘ Trojan.GenericKD.62095134

113. The configuration file stored within the downloaded archive was not flagged as potential malware.

114. Detection by these vendors does not conclusively indicate that the analyzed resource is or is not malware. Detection criteria are specific to the vendor providing the detection, but commonly involve decompilation of submitted resources for static analysis as well as execution of resources for dynamic analysis, where possible. From this combination of analysis methods, the behavior of a potential piece of malware may be observed and classified.

115. Therefore, while the VirusTotal detections do not definitively identify the AimJunkies loader as traditional malware, they do clearly show that the way the loader behaves when it is active on a user's device behaves like traditional malware, and may be used to facilitate the installation and

Client Confidential

operation of malware. These detections are also the probable reason for AimJunkies' instructions to add exceptions to or disable security features in advance of loader installation. Leaving these features untouched would almost certainly result in the downloaded .zip archive and the loader inside it to be quarantined and removed from the device.

116. Finally, even if the AimJunkies loader itself is not malware, and does not directly harm a user or their device, it represents a clear and present danger to the user the moment it is successfully downloaded and installed – even on a USB flash drive, as AimJunkies suggests. Installing the Aimjunkies software according to the vendor's instructions immediately leaves the user's computer vulnerable to infection by viruses, trojans, and ransomware. In a potential worst-case scenario, the cheat publishers themselves would be able to gain full administrative access to a user's computer with trivial effort.

AimJunkies Cheat: General Inferences

117. Microsoft Windows uses a set of core libraries containing code for basic actions the operating system may perform. For example, a system library can contain the functions that read from a file, that register mouse or keyboard input, or that send data over the network. One way cheat software functions is to require the cheat process to inject itself, or "hook," into one of these basic actions. Once this is done, when the *Destiny 2* game client attempts to perform a modified system action, it causes the installed cheat to execute as well. Cheat loaders need to be run with administrative access in order to hook into system libraries. Another way for cheat software to function is for the cheat process to inject itself or to "hook" into the game client process. Video game developers use numerous techniques to block the manipulation of system core libraries, and cheat software must circumvent those protections in order for the cheat software to function.
118. The *Destiny 2* program resides on disk before it executes. When launched by the user, the program then copies itself into memory. Each program has its own designated space in memory, and programs typically cannot access the memory space of another program. However, system libraries are considered to be trusted, and, because the injected cheat is hooked to an action in the system library, it, too, gains access to the *Destiny 2* disk space. When the *Destiny 2* client program calls the function that the cheat is hooked to, the cheat executes with the ability to read and modify *Destiny 2* memory.
119. As described in Section 48, each *Destiny 2* player has a local copy of the game state. This game state contains all of the information available to the player through in-game displays, as well as information that is meant to be hidden from the player. The game client determines what information to provide to the player. For example, the game client knows when another player is on the other side of a wall. The game client allows the player to see the wall, but not the player on the other side of the wall. It intentionally obscures that information from the player. However, AimJunkies and other similar cheats can read this information out of the game client's memory and display it to the cheater to grant an advantage.
120. The cheat projects graphical elements onto the visual display of the *Destiny 2* program containing this information. This type of display modification almost always requires that the

Client Confidential

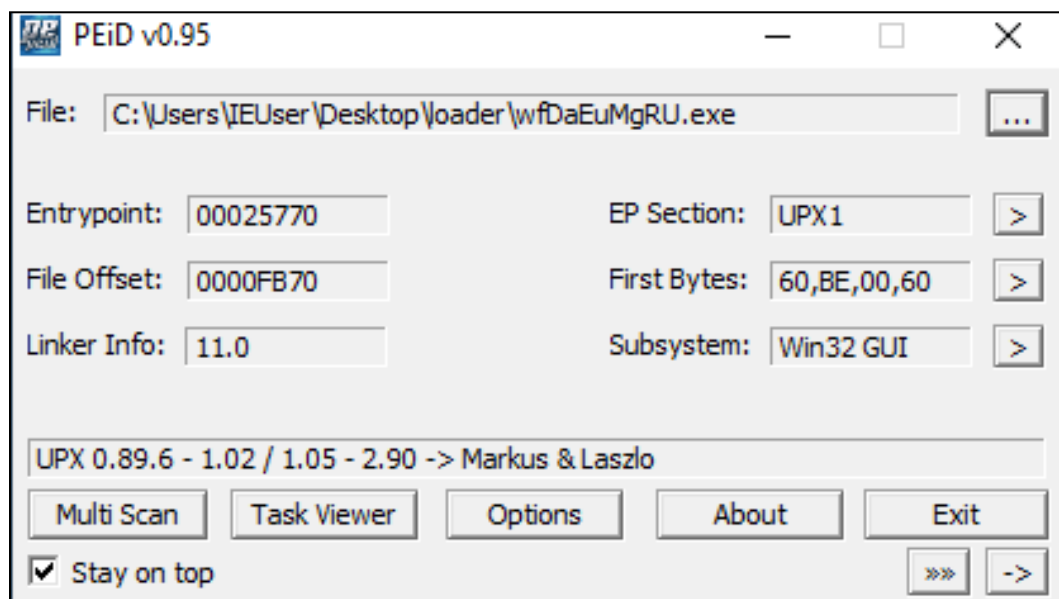
cheat software hook the game software's rendering functions. As seen in the image below, this commonly includes highlighted boxes that show the locations of other players' Guardians, even when the cheating player's Guardians should not be able to see them.



121. The ability to know the location of other players' Guardians when they should be hidden from sight provides a clear and significant advantage to the cheating player. The cheater gains the element of surprise over the non-cheating player and has the ability to shoot first, which is crucial in a first-person shooter.
122. Cheats may also manipulate the client to simulate user inputs, or even perform game actions directly. The aimbot functionality provided by the AimJunkies *Destiny 2* cheat appears to read the positions of other players or NPC enemies from the client's game state data, and then automatically moves the player's Guardian to aim perfectly at the target's head for a guaranteed headshot critical hit.
123. More specifically, the aimbot functionality appears to read the relative locational data of opposing Guardians from the game client's data on the current game state, and then uses this data to determine what mouse movements would be required for the cheater to register a headshot critical hit on their target. The cheat uses this data to tell the cheater's computer that this movement has been made as a simulated input, separate from the cheater's own mouse movements. The computer receives this instruction from trusted system functions, and therefore passes this instruction to the game client as the cheater's legitimate input. The game client, trusting these instructions from the computer, receives this input and performs the corresponding actions.
124. Again, this cheat appears to operate by reading data from the *Destiny 2* memory and accordingly manipulating the user's device.
125. Aiming is a game skill typically honed over the course of years. It is one of the fundamental ways *Destiny 2* players compete with one another. Skilled players can perform incredibly precise movements to hit difficult shots, but players using aimbots can obtain perfect accuracy with the click of a mouse. By removing the skill element from this core game mechanic, cheaters degrade the competitive spirit that draws many players to *Destiny 2*.

Client Confidential**AimJunkies Loader Dynamic Analysis and Reverse-Engineering**

126. Over the week of November 14, 2022, I and members of Unit 221B's offensive engineering team performed dynamic malware analysis on the AimJunkies loader. This analysis included examination of the loader's behavior during and after the installation process detailed above, as well as partial reverse-engineering.
127. The AimJunkies loader, also known as the OverDose loader, is a 32-bit Windows Portable Executable file (or PE, with file extension .exe). This PE is packed using the UPX packer,³⁰ an open source utility designed to reduce PE file size and obfuscate program code from the casual observer. Although UPX has legitimate uses, it is commonly seen in the context of malware executables.



128. The AimJunkies loader PE appears to be arbitrarily assigned a random string of characters as its filename on download, resulting in each user having a differently named, yet functionally identical, file. The version of the loader collected by Unit 221B on September 15, 2022, uses the name **wfDaEuMgRU.exe**, with an accompanying configuration file **wfDaEuMgRU.cfg**.

Name	Type
 wfDaEuMgRU.cfg	Configuration Source File
 wfDaEuMgRU.exe	Application

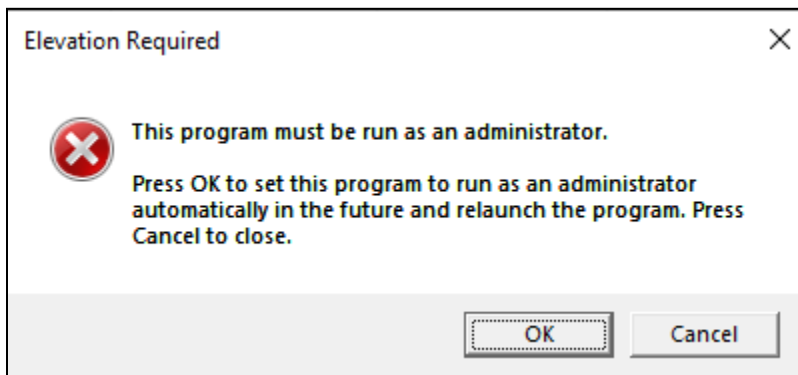
129. I attempted loader installation in both a malware analysis sandbox virtual machine as well as direct hardware on a quarantined device. Despite multiple attempts and different system configurations, I was unable to install the AimJunkies loader within the sandbox environment.

³⁰<https://upx.github.io/>

Client Confidential

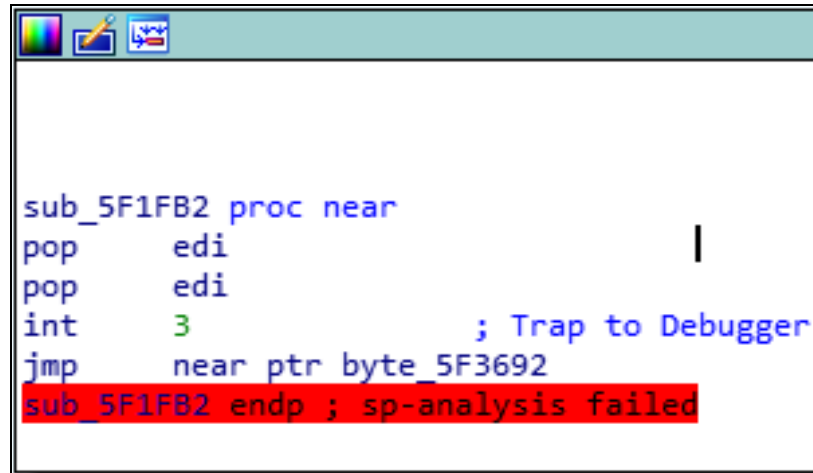
Later analysis revealed that the loader uses Windows system hooks to check for the presence of a virtual machine, killing loader processes if one is detected. Such obfuscation methods are common in malware distributions and serve to frustrate attempts to unpack and reverse-engineer the program in question. I successfully installed the AimJunkies loader directly onto the home system of a quarantined device, allowing for further dynamic analysis of the PE.

130. As noted in the installation instructions, the AimJunkies loader must be run with administrative privileges. Administrator permissions are required to alter the Windows Registry entries, disable antivirus and protection features, and simulate user input using Windows system hooks. These functions are required by the AimJunkies loader to function. Administrator-level permissions are required to interact with other administrator-level programs and core system functions. Running the loader with this level of privilege acts as a protective measure to prevent the loader from being flagged, quarantined, and removed as malware by basic system protections.



131. The loader appears to be written in the C++ programming language. It launches two processes in sequence. In this context, a process or thread may be considered as an execution path of the original code to launch the software. One of these processes appears to be designed as a trap to stymie debugging and reverse-engineering attempts. If the original PE is run to completion while loaded within a debugger, the debugger will observe this first process as completed well before the second. If that happens, the debugger will consider the entire program terminated at this completion point. Meanwhile, the second process continues to run unobserved by the debugging utility.
132. This type of obfuscation is referred to as an “escape-based” technique. It is intended to frustrate debugging and reverse-engineering attempts. The loader appears to use a common evasion technique of setting “int 3” as a “debugger trap.”³¹ This assembly instruction causes a program exception which is ignored when a debugger is not present, but creates a terminal breakpoint when the software is run through a debugger.
133. An example of this “trap” may be seen in the image below captured from the unpacked Aimjunkies loader as observed in a debugging application. Inclusion of the line “int 3,” annotated by the debugging software as “Trap to Debugger,” forces an error within the debugging application, as displayed by the red highlight text following this instruction.

³¹<https://anti-debug.checkpoint.com/techniques/assembly.html>

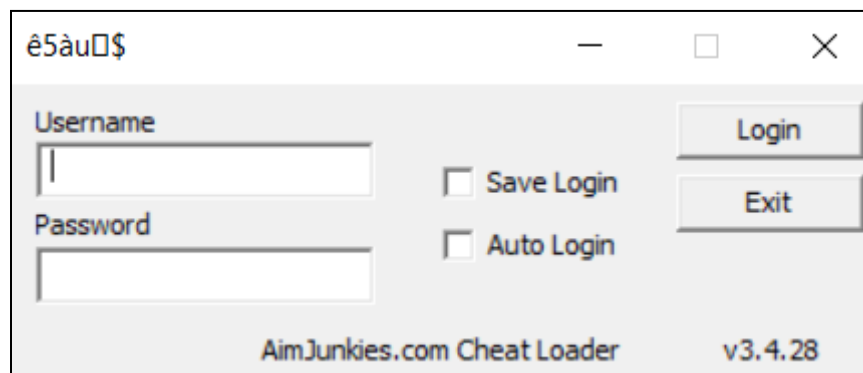
Client Confidential


```

sub_5F1FB2 proc near
pop      edi
pop      edi
int      3          ; Trap to Debugger
jmp      near ptr byte_5F3692
sub_5F1FB2 endp ; sp-analysis failed

```

134. On execution, this second process installs and initializes the AimJunkies loader, prompting the user for their AimJunkies credentials. These credentials are verified against the AimJunkies server, after which the user is presented with a menu of options for available cheats. The window title for the loader is an random string, which changes on each execution and appears to be randomly generated to prevent program signature detection



135. Upon execution of this second process, the AimJunkies loader uses a technique known as “DLL side-loading”³² to inject itself into the Microsoft Internet Explorer application. Although Microsoft has transitioned their browser offering from Internet Explorer to the newer Microsoft Edge, Internet Explorer remains a standard application packaged alongside relatively recent installations of Microsoft Windows. Microsoft officially ended support for Internet Explorer on June 15, 2022,³³ which means it will no longer receive regular maintenance or security patches. Software in this state is commonly exploited by malware to take advantage of the trusted nature of the software to disguise malicious activity, as appears to be the case with the AimJunkies loader.
136. The AimJunkies loader appears to use an architecture-based circumvention method in this process to further avoid debugging and other reverse-engineering efforts. As previously noted,

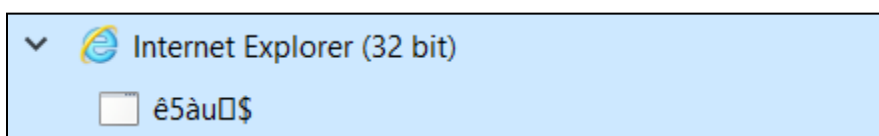
³²<https://attack.mitre.org/techniques/T1574/002/>

³³<https://support.microsoft.com/en-us/microsoft-edge/make-the-switch-to-microsoft-edge-a6f7173e-e84a-36a3-9728-3df20ade9b3c#:~:text=Support%20for%20Internet%20Explorer%2011%20has%20ended%20on%20June%2015%2C%202022&text=Micr osoft%20Edge%20is%20the%20faster.to%20know%20with%20Internet%20Explorer.>

Client Confidential

the AimJunkies loader is a 32-bit PE application; the Internet Explorer instance exploited by the loader is also a 32-bit application. Injection of 32-bit code into a trusted application space allows for hiding execution and memory loading within the injected application. By using iexplore.exe as the application to inject into, it complicates reverse engineering as it forces the engineer to sift through Internet Explorer's application along with identifying the injected code.

137. After execution and hijacking of the Internet Explorer process, the AimJunkies loader displays as a legitimate "iexplore.exe" process on the user's system. This technique is likely the root cause of many of the Virustotal detections for this file. After finalizing injection, the loader calls multiple standard Windows system libraries. It uses these to create the user interface, open connections between the user's device and the AimJunkies backend, and support system calls that allow installation and continued modification of the system based on specific cheat requirements.



138. These system calls suggest the loader software conducts most of the activities associated with the cheat such as the aimbot or ESP features advertised by AimJunkies. Game-specific cheat files likely direct the loader to the memory spaces used by a game such as *Destiny 2* during operation, allowing the loader to illegitimately read game state data from memory. However, as the AimJunkies *Destiny 2* cheat is unavailable on the AimJunkies store and has not been provided by AimJunkies for analysis, this conclusion is a theory based on observable evidence.
139. Once the application is closed, an unauthenticated instance of the loader appears to leave no trace on the user's device aside from the initially downloaded executable. However, configuration changes made by the user to their antivirus, firewall, and user account control settings remain and represent a significant vulnerability to the affected device.
140. Therefore, the AimJunkies loader is not overtly destructive, but allows for the download of unknown applications that have full administrator privileges and complete control of the infected device, its system libraries, and its executables. By hijacking the Internet Explorer application, the loader actively attempts to hide itself from the operating system and frustrate attempts to reverse-engineer, unpack, or debug the loader executable.

Game Product Devaluation

141. The presence of cheaters within a game environment poisons the well for legitimate players and devalues the larger ecosystem built up around an online live-service multiplayer game such as *Destiny 2*.
142. The presence of cheaters within this ecosystem has other knock-on effects. Cheaters produce negative reactions from the community on social media and discourage content creators from featuring the game on streams and recorded video. This negative reaction also disincentivizes developers from community interaction, which in turn leads to angrier fans. The social media feedback loop becomes a vicious circle.


Client Confidential

143. *Destiny 2*'s success is defined by aspirational and difficult content, or "endgame" content, that players are intended to enjoy through hundreds or thousands of hours to come. This content is accessed typically by players who have invested significant amounts of time and money in their characters, and who frequently have worked hard to improve their skill at the game. Cheating allows players to skip this investment, immediately becoming more successful than any other player.
144. Even where a cheat developer's customers only make up a small fraction of the game's player community, their effect on the community is significant. For instance, in a live-service online multiplayer game like *Destiny 2*, retention of invested players is paramount for Bungie. Competitive PvP and other endgame activities concentrate invested players at the highest levels, making it nearly inevitable that players who have invested the most time for skill building within the game will encounter cheaters more frequently than the rest of the player community. If these players are blocked from completing endgame activities by constant interactions with cheaters, they will choose to invest their time and money elsewhere. Those high-level players are often a large driving force of the popularity of a game, and when they leave a game, its popularity (including player count and social media presence) drops as well.
145. Cheating has also given rise to cottage industries built around online games by third parties, which may collectively be referred to as "boosting services." Boosting services provide a shortcut to success by fraudulently logging into another player's account and playing on their behalf, or else transferring items to a player in exchange for real-world money. The scale of these boosting services is enabled by access to cheats, which allow these boosters to provide returns to their customers rapidly and move on to the next order. In its purest form, paying for a boosting service is paying for someone else to cheat for you.
146. Unlike casual cheat users, boosting service operators have a financial incentive to play *Destiny 2* using cheat software constantly. Common goals of boosting service operators include such tasks as leveling a character rapidly to have it prepared for endgame activity for the account owner; or "farming" repeatable activities, such as the endgame PVP mode "Trials of Osiris," to acquire in-game titles (like "Flawless") or rare "loot." The prevalence of boosting services increases the likelihood that legitimate players will encounter and will be negatively impacted by cheat software users.
147. When legitimate players of *Destiny 2* are forced into interactions with cheaters of any variety, the game quickly begins to lose value for them. The highest tiers of play and reward become inaccessible, and continue to grow more inaccessible as players avoid the game out of fear and disgust when they encounter cheaters. Unimpeded cheat software represents a fundamental shift in the end-state of the game, with spiraling consequences that threaten the health of the game itself, causing harm to Bungie.

Client Confidential

Conclusion

148. Bungie's *Destiny 2* game is buoyed by an active and engaged player community that participates in organic social media marketing and thrives on content from creators who promote *Destiny 2* to them and for them.
149. This engagement relies upon the healthy and fair in-game environment Bungie provides, an environment which ensures that player success is defined by skill and dedication to the game. Bungie has a clear security commitment to their players to maintain this environment.
150. The presence of cheaters within this environment damages Bungie and devalues the game for everyone involved. Fans are unhappy, unhappy fans discourage content creators from featuring the game, and developers are less likely to engage with the community.
151. Cheaters seek to "pay-to-win," bypassing skill-building and time investment by purchasing unauthorized third-party software to ensure their success.
152. Cheat software threatens users. Vendors instruct users to disable security features or otherwise block them from interacting with their software, laying them open to attacks by viruses, trojans, and malware. A wide array of security providers detected the AimJunkies cheat loader as potential malware.
153. Cheat software appears to interact with the *Destiny 2* game client in unauthorized ways to provide cheaters competitive advantages against legitimate players.
154. Dynamic and static analysis conducted on the AimJunkies loader reveals malicious and problematic behavior on the part of the loader that represents a clear and present danger to users of AimJunkies cheats. While not malware in and of itself, the loader makes use of multiple evasion and circumvention techniques most commonly seen in malware executables.
155. The continued presence of cheaters in the *Destiny 2* game environment devalues the game by preventing legitimate players from achieving endgame goals that reflect their personal investments of time and energy and money. Dissatisfied players will leave *Destiny 2* and spend their time and money elsewhere, with Bungie.



Steven Guris